(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日:
2005年8月18日(18.08.2005)

PCT

(10) 国际公布号:
WO 2005/076517 A1

(51) 国际分类号[7]: H04L 9/08

(21) 国际申请号: PCT/CN2004/000969

(22) 国际申请日: 2004年8月19日(19.08.2004)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200410013996.6 2004年2月2日(02.02.2004) CN

(71) 申请人(对除美国以外的所有指定国): 中国科学技术大学(UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA) [CN/CN]; 中国安徽省合肥市金寨路96号, Anhui 230026 (CN)。

(72) 发明人;及
(75) 发明人/申请人(仅对美国): 韩正甫(HAN, Zhengfu) [CN/CN]; 朱冰(ZHU, Bing) [CN/CN]; 莫小范(MO, Xiaofan) [CN/CN]; 郭光灿(GUO, Guangcan) [CN/CN]; 中国安徽省合肥市金寨路96号, Anhui 230026 (CN)。

(74) 代理人: 中科专利商标代理有限责任公司(CHINA SCIENCE PATENT & TRADEMARK AGENT LTD); 中国北京市海淀区王庄路1号清华同方科技大厦B座15层, Beijing 100083 (CN)。

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW

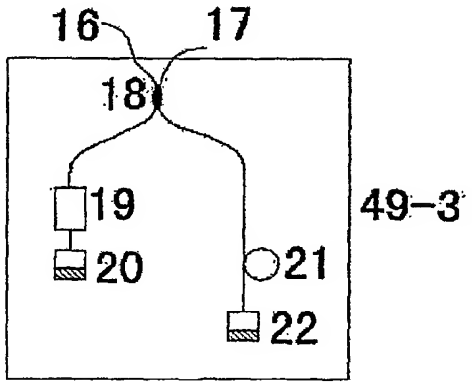
(84) 指定国(除另有指明, 要求每一种可提供的地区保护): ARIPO(BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚专利(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲专利(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

本国际公布:
— 包括国际检索报告。

所引用双字母代码和其它缩写符号, 请参考刊登在每期PCT公报期刊起始的"代码及缩写符号简要说明"。

(54) Title: A POLARISATION-CONTROLLED ENCODING METHOD, ENCODER AND QUANTUM KEY DISTRIBUTION SYSTEM

(54) 发明名称: 一种偏振控制编码方法、编码器和量子密钥分配系统



(57) Abstract: The invention relates to a polarisation-controlled encoding method, encoder and quantum key distribution system according to the invention and characterized in that polarisation maintaining light path or 90 degree rotation Faraday mirror are used inside the encoder to keep the polarisation of the output pulses same, and that in the quantum key distribution system employing the polarisation-controlled encoder the pulse emitted from transmitter unidirectionally transmits to receiver and then quantum key distribution is implemented using interference in the pulses according to the quantum key distribution protocol. The quantum key distribution system using the polarisation-controlled encoder of the invention has the ability of anti-wiretapping to transmitter, receiver and quantum channel. Detection units each of which separates reversed photon from other photons are added at the out port of the transmitter and the in port of receiver, respectively, so that Trojan horse is prevented from entering and photons with phase modulated information are prevented from leaving the safe area in receiver. Unconditionally safe key distribution can be accomplished by using the quantum key distribution system of the invention

[见续页]

WO 2005/076517 A1

(57) 摘要

本发明的偏振控制编码方法、编码器和量子密钥分配系统，特征是在编码器内部采用偏振保持光路或 90 度旋转法拉第反射镜反射使输出光脉冲偏振态相同；以偏振控制编码器为核心组成的量子密钥分配系统，发送端输出的光脉冲经量子信道单向传给接收端，根据光脉冲的叠加干涉结果，按照量子密钥分配协议实现量子密钥分配。本发明的偏振控制编码器使得系统具有抗发送装置、接收装置和量子信道中的干扰的能力，在系统的发送装置的出口和接收装置的入口增加反向光子分离检测单元，阻止了木马光子的入侵和携带调制信息的光子离开接收装置的安全区。利用本发明的量子密钥分配系统，可以实现密钥的无条件安全分配。

一种偏振控制编码方法、编码器和量子密钥分配系统

技术领域

本发明属于光传输保密通信技术领域，特别涉及量子密钥分配中的编码方法和装置。

背景技术

早期的量子密钥分配用光子偏振编码，这种方式适合于自由空间通信而不适合于光纤通信体系。因为普通光纤对称性不是很好、传输路径中的干扰表现为对光的偏振状态的影响，所以无法保持光在其中传播时的偏振态，偏振编码也就不适合在光纤中使用。美国专利号 5307410 公布了一种用一对不等臂马赫-曾特（Mach-Zehnder）干涉仪为基础的相位编码量子密钥分配方案，其接收和发送装置内的光脉冲分别经历马赫-曾特干涉仪的不同臂，因为不同臂受到的干扰不可能完全一致，无法互相完全抵消，因此稳定性不好，抗干扰能力差；又因为两个光子脉冲分别通过马赫-曾特干涉仪的不同臂经历了不同光路，进入量子信道时两个脉冲的偏振状态不能保证确定关系，因此对量子信道中的干扰很敏感，长程量子密钥分配时这种干扰尤为严重，该方案的多种变化版本均无原则性的改进。

鉴于双不等臂 M-Z 干涉仪方案存在的稳定性问题，美国《应用物理快报》（Appl. Phys. Lett. 77（7），793（1997））提出了一种解决方案，用法拉第反射镜使两个光脉冲在发送和接收点之间传输一个来回，每个光脉冲经过所有光路一次，达到了自补偿的效果。此方案假定光子脉冲来回两次历经同一位置时干扰信号来不及变化，光脉冲所受干扰一致，叠加时干扰效果互相抵消从而达到抗干扰和稳定的目的。而事实上，这种稳定只在传输距离不太长和干扰频率不太高时有效，当传输距离增大时，光脉冲来回经历同一位置的时间差增加，抗干扰能力也就随之降低；另外，由于光脉冲要在量子信道中来回两次，信道总损耗等于实际量子信道两倍长度时的损耗，通常采用去程强光和回程单光子的方法弥补这种缺陷，但这种弥补方法只适用于目前的以强衰减激光脉冲模拟单光子源的情况，理想量子密钥分配的光源应是单光子源，但目前理想单光子源还不能实用，一旦使用理想单光子源，这种方案的极限传输距离只有现在的一半；一个更加严重的缺陷是这种方案潜藏了安全隐患：窃听者可能将进入接收区前

的强信号按比例衰减，再用波长与工作波长非常接近的木马信号补充，使得接收区内的总监测信号强度不变，即信号强度监测失效，当信号返回时，木马信号可被窃听者分离并检测出所携带的信息，再将原始信号光子由“超级低损耗信道”传回发送者，只要窃听者适当控制信号衰减比例，就可以做到系统的接收码率不受影响，从而不被发送者发现。对信息安全技术来说，这种可窃听的隐患是致命的。

发明内容

本发明提出一种偏振控制编码方法、根据该方法构造的偏振控制编码器以及由这种编码器组成的量子密钥分配系统，可以在两个用户间形成一组不被窃听的量子密钥，实现密钥的无条件安全分配。

本发明的偏振控制编码方法，其特征在于将入射的一个光脉冲分束为两个光脉冲，对二者作相对延时，再使这两个脉冲合成为一路输出，并在分束或合束后对其中的至少一个光脉冲按量子密钥分配协议进行相位调制，即编码；在分束到合束的过程中控制输出的两个光脉冲的偏振态，使得合束后输出的这两个光脉冲的偏振态相同。

所述使得合束后输出的这两个光脉冲的偏振态相同的控制方式，可以是使两个光脉冲从分束到合束过程中的偏振状态保持不变；或使两个光脉冲分别经 90 度旋转法拉第反射镜反射奇数次，并经历分束到合束的各自的光路偶数次；或使两个光脉冲之一直接输出，另一经 90 度旋转法拉第反射镜反射偶数次，并经历分束到合束的各自的光路偶数次。

根据本发明的偏振控制编码方法构造的第一种偏振控制编码器，其特征在于将一个光脉冲经过一个偏振保持分束器后分成两个光脉冲沿两条光路传播，其中任一光路由延时线相对另一光路延时后再由偏振保持分束器合成为一条光路输出，所述分束后的两条光路和合束后的输出光路三者中至少一路有相位调制器，所述偏振保持编码器的内部光路在分束到合束之间的部分是偏振保持光路。

根据本发明的偏振控制编码方法构造的第二种偏振控制编码器，其特征在于将一个光脉冲经过一个偏振保持分束器后分成两个光脉冲沿两条光路传播，分别由反射镜反射回来，其中任一光路的反射镜前加入延时线，使两条光路之间相对延时，并由原偏振保持分束器合成为一条光路输出，所述分束后的两条光路和合束后的输出光路三者中至少一路有相位调制器，所述偏振保持编码器的内部光路在分束到合束之间的部分是偏振保持光路。

根据本发明的偏振控制编码方法构造的第三种偏振控制编码器；其特征在于将一个光脉冲经过一个分束器后分成两个光脉冲沿两条光路传播，并分别由 90 度旋转法拉第反射镜反射回来，其中任一光路中的 90 度旋转法拉第反射镜前加入延迟线，使这两个光脉冲相对延时，再由原分束器合成为一条光路输出，所述分束后的两条光路和合束后的输出光路三者中至少一路有相位调制器。

根据本发明的偏振控制编码方法构造的第四种偏振控制编码器，其特征在于将一个光脉冲经过一个偏振保持可变分束器后分成两个光脉冲沿两条光路传播，一路直接输出，另一路由反射镜反射回来，并经过原偏振保持可变分束器后再由反射镜反射回来，再经过原偏振保持可变分束器与上述直接输出光脉冲合成为一条光路输出，所述反射镜前的两条光路中至少一个有延时线，所述反射镜前的两条光路和合束后的输出光路三者中至少一路有相位调制器，所述延时线与相位调制器在同一光路中时先后位置可以互易，所述偏振保持编码器的内部光路在分束到合束之间的部分是偏振保持光路。

根据本发明的偏振控制编码方法构造的第五种偏振控制编码器，其特征在于将一个光脉冲经过一个可变分束器后分成两个光脉冲沿两条光路传播，一路直接输出，另一路由 90 度旋转法拉第反射镜反射回来，并经过原可变分束器后再由 90 度旋转法拉第反射镜反射回来，再经过原可变分束器与上述直接输出光脉冲合成为一条光路输出，所述 90 度旋转法拉第反射镜前的两条光路中至少一个有延时线，所述 90 度旋转法拉第反射镜前的两条光路和合束后的输出光路三者中至少一路有相位调制器，所述延时线与相位调制器在同一光路牛时先后位置可以互易。

本发明的量子密钥分配系统，其特征在于将从脉冲光源输出的一个光脉冲经发送端的偏振控制编码器分束成两个光脉冲沿两条光路传播，对二者作相对延时，再使这两个脉冲合束成一路输出，并在分束或合束后对至少一个光脉冲按量子密钥协议约定进行相位调制，偏振控制编码器输出的这两个光脉冲经过量子信道单向传给接收端，接收端的偏振控制编码器将接收到的这两个光脉冲中的每个光脉冲分束成两个光脉冲组成的光脉冲组沿两条光路传播，对同组的二个光脉冲按量子密钥协议约定作相对延时，再使这两组光脉冲合束成一路输出，并按量子密钥协议约定进行相位调制，用单光子探测器同步检测这两组光脉冲中各至少一个光脉冲的叠加干涉结果，根据量子密钥分配协议实现量子密钥分配；当上述五种偏振控制编码器任一种用于接收端且其中的相位调制器位于输出光路时，需将该相位调制器移至脉冲分束前的输入光路中。

可以在该量子密钥分配系统的发送装置的出口或接收装置的入口串接反向光子分离检测单元，反向光子分离检测单元由光环行器和单光子探测器组成，其中光环行器的输入端接偏振控制编码器的输出端，环行器的同向输出端接量子信道，反向输出端接单光子探测器的输入端，增加反向光子分离检测单元可以阻止木马光子的入侵并阻止携带调制信息的光子离开接收装置的安全区。还可以在所述的反向光子分离检测单元中的光环行器的输入端串接一个光学带通滤波器，以弥补光环行器和单光子探测器的响应带宽不足。

所述量子信道，可以是光波导、光纤、自由空间，分立光学元件或它们中任意两个以上组合成的光传播通道。

与现有双不等臂马赫-曾特于涉仪组成的编码器相比较，由于本发明的偏振控制编码器在其内部控制光脉冲的偏振态，首先使得编码器对自身所受的于扰不敏感，量子密钥分配系统对环境的要求大大降低；同时由于进入量子信道的两个光脉冲间的偏振态相同，使得光脉冲在共同路径中所受的干扰在接收端叠加干涉时互相抵消，实现了信号传输与信道干扰无关，大大提高了系统的实际稳定性；在本发明的 90 度旋转法拉第反射镜式偏振控制编码器中，由于光脉冲两次经过相位调制器，且通过时的偏振方向互相垂直，只要相位调制信号持续时间长于光脉冲来回两次经过的时间，则相调制大小与光脉冲的偏振状态无关，因此可用偏振相关的相位调制器达到偏振无关相位调制的目的，且对相位调制器的速度要求也可以降低；在本发明的以偏振保持分束器组成的偏振控制编码器中，由于光脉冲均被保持在特定的偏振态上，偏振相关的相位调制器自然适用。

在本发明的量子密钥分配系统中，发送端和接收端可以增加反向光子分离检测单元，在增加了反向光子分离检测单元后，由于信号光脉冲从发送装置单向通过量子信道传输到接收装置，可将任何反方向传输的光子分离出来并导入单光子探测器进行检测，这样不仅可以阻止可能的木马光子进入编码器携带出编码信息，而且可以知道是否有窃听者存在，杜绝了被木马攻击的可能；考虑到单光子探测器和环行器工作波长有一定范围，本发明的量子密钥分配系统中可以增加光学带通滤波器，系统工作范围内的光脉冲可以通过，工作范围以外波长的光不能通过，弥补单光子探测器和环行器工作波长范围不够宽的缺点。

附图说明

图 1 为偏振保持光路马赫-曾特干涉仪式偏振控制编码器的基本组成示意图；

图 2 为偏振保持光路反射镜式偏振控制编码器的基本组成示意图；

图 3 为 90 度旋转法拉第反射镜式偏振控制编码器的基本组成示意图；

图 4 为 90 度旋转法拉第反射镜式偏振控制编码器的变化型的基本组成示意图；

图 5 为相位调制器位于输出光路的 90 度旋转法拉第反射镜式偏振控制编码器的基本组成示意图；

图 6 为使用可变分束器的偏振保持光路反射镜式偏振控制编码器的基本组成示意图；

图 7 为使用可变分束器的 90 度旋转法拉第反射镜式偏振控制编码器的基本组成示意图；

图 8 一种反向光子分离检测单元；

图 9 为另一种增加带通滤波器的反向光子分离检测单元。

图 10 为以偏振控制编码器为核心的相位调制光纤量子密钥分配系统结构示意图。

具体实施方式

实施例 1：

本发明的量子密钥分配系统中的偏振控制编码器的第一种组成结构如图 1 所示：它由两个 2×2 的 3dB 偏振保持分束器 3、6，一个偏振保持相位调制器 5 和一个偏振保持延时线 4 组成，共同构成一个偏振保持马赫-曾特干涉仪。其中 3dB 偏振保持分束器 3 的一侧的两端口 1 和 2 之一作为偏振控制编码器的输入端，3dB 偏振保持分束器 6 的另一侧的两端口 7、8 之一作为输出端，偏振保持相位调制器 5 和偏振保持延时线 4（顺序任意）一起插入上述马赫-曾特干涉仪的任一个臂，或二者分别插入上述马赫-曾特干涉仪的二个臂。工作时，光脉冲经偏振保持分束器 3 的端口 1 或 2 进入偏振保持分束器 3 分成两路，一路经过偏振保持相位调制器 5 进行相位调制，另一路经过偏振保持延时线 4 延时，相对延时后的两路经偏振保持分束器 6 合成一路由端口 7 或 8 输出，因所有光路均为偏振保持光路，所以由此输出的两个脉冲的偏振态相同。当偏振保持相位调制器 5 和偏振保持延时线 4 位于偏振保持马赫-曾特干涉仪的同一臂时，上述结果不受影响。

实施例 2：

本发明的量子密钥分配系统中的偏振控制编码器的第二种组成结构如图 2 所示：它由一个 2×2 的 3dB 偏振保持分束器 11、两个反射镜 13 和 15、一个偏振保持相位调制器 12 和一个偏振保持延时线 14 组成。其中 3dB 偏振保持分束器 11 的一侧的两端口 9 和 10 均可作为偏振控制编码器的输入和输出端，3dB 偏振保持分束器 11 的另一侧的两端口之一依次连接偏振保持相位调制器 12、反射镜 13，同侧另一端口则顺序连接偏振保持延时线 14、反射镜 15，一种略有变化但功能相同的结构是将偏振保持延时线 14 与偏振保持相位调制器 12（顺序无关）同时串接在同一端口，而另一端口仅连接一个反射镜。工作时，光脉冲经偏振保持分束器 11 的端口 9 进入偏振保持分束器 11 分成两路，一路经过偏振保持延时线 14 延时，由反射镜 15 反射回来，另一路经偏振保持相位调制器 12 进行相位调制后再经反射镜 13 反射回来，反射回来的两路光脉冲经偏振保持分束器 11 合成一路由端口 10 输出，因所有光路均为偏振保持光路，所以由 10 输出的两个脉冲的偏振态相同。当偏振保持延时线 14 和偏振保持相位调制器 12（顺序无关）串接在同一端口，而另一端口仅连接一个反射镜时，上述结果不受影响。光脉冲从 10 端口输入，9 端口输出和以端口 9 或 10 同时作为输入和输出时结果相同。

实施例 3：

本发明的量子密钥分配系统中的偏振控制编码器的第三种组成结构如图 3 所示：它由一个 2×2 的 3dB 分束器 18、两个 90 度旋转法拉第反射镜 20 和 22、一个相位调制器 19 和一个延时线 21 组成。其中 3dB 分束器 18 的一侧的两端口 16 和 17 分别作为偏振控制编码器的输入和输出端，3dB 分束器 18 的另一侧的两端口之一依次连接相位调制器 19、90 度旋转法拉第反射镜 20，同侧另一端口则顺序连接延时线 21、90 度旋转法拉第反射镜 22。工作时，光脉冲经分束器 18 的端口 16 进入分束器 18 分成两路，一路经过延时线 21 延时，由 90 度旋转法拉第反射镜 22 反射回来，另一路经相位调制器 19 进行相位调制后再经 90 度旋转法拉第反射镜 20 反射回来，反射回来的两路光脉冲经分束器 18 合成一路由端口 17 输出，因两条光路均经 90 度旋转法拉第反射镜反射并经历各自的光路偶数次，所以由此输出的两个脉冲的偏振态相同。光脉冲从 17 端口输入，16 端口输出和以端口 16 或 17 同时作为输入和输出时结果相同。

实施例 4：

另一种结构略有变化但功能相同的偏振控制编码器如图 4 所示，差别在于将相位调制器 19、延时线 21、90 度旋转法拉第反射镜 22 顺序连接在耦合器的一个端口上（其

中 19 和 21 的顺序可以互易），另一端口上只连接一个 90 度旋转法拉第反射镜 20。工作时，光脉冲经分束器 18 的端口 16 进入分束器 18 分成两路，一路经相位调制器 19 进行相位调制再经过延时线 21 延时（顺序无关）后，由 90 度旋转法拉第反射镜 22 反射回来，另一路由 90 度旋转法拉第反射镜 20 反射回来，反射回来的两路光脉冲经分束器 18 合成一路由端口 17 输出，因两条光路均经 90 度旋转法拉第反射镜反射并经历各自的光路偶数次，所以由此输出的两个脉冲的偏振态相同。光脉冲从 17 端口输入，16 端口输出和以端口 16 或 17 同时作为输入和输出时结果相同。

实施例 5：

本发明的量子密钥分配系统中的偏振控制编码器的第四种组成结构如图 6 所示：它由一个 2×2 的偏振保持可变分束器 25、两个反射镜 23 和 27、一个偏振保持相位调制器 24 和一个偏振保持延时线 26 组成。其中偏振保持可变分束器 25 的一侧的两个端口之一作为偏振控制编码器的输出端 28，另一端口经偏振保持延时线 26 接反射镜 27；偏振保持可变分束器 25 的另一侧的两个端口之一作为偏振控制编码器的输入端 29，另一端口经偏振保持相位调制器 24 接反射镜 23。一种略有变化但功能相同的结构是将偏振保持延时线 26 与偏振保持相位调制器 24（顺序无关）串接在同一端口，而另一端口仅连接一个反射镜。工作时，光脉冲经偏振保持可变分束器 25 的端口 29 进入偏振保持可变分束器 25 分成两路，一路直接从偏振保持可变分束器 25 的端口 28 直接输出，另一路经过偏振保持延时线 26 延时，由反射镜 27 反射回来，再经过偏振保持可变分束器 25，再经过偏振保持相位调制器 24 进行相位调制后经反射镜 23 反射回来，反射回来的光脉冲经偏振保持可变分束器 25 与上述直接输出的光脉冲合成一路由端口 28 输出，在对光脉冲进行分束时，控制偏振保持可变分束器的分束比，使得由端口 28 输出的两个光脉冲幅度相等，因所有光路均为偏振保持光路，所以由此输出的两个光脉冲的偏振态相同。当偏振保持延时线 26 和偏振保持相位调制器 24（顺序无关）串接入同一端口，而另一端口仅连接一个反射镜时，上述结果不受影响。脉冲从 28 端口输入，29 端口输出时结果相同。

实施例 6：

本发明的量子密钥分配系统中的偏振控制编码器的第五种组成结构如图 7 所示：它由一个 2×2 的可变分束器 32、两个 90 度旋转法拉第反射镜 30 和 34、一个相位调制器 31 和一个延时线 33 组成。其中可变分束器 32 的一侧的两个端口之一作为偏振控制编码器的输出端 35，另一端口经延时线 33 接 90 度旋转法拉第反射镜 34；可变

分束器 32 的另一侧的两个端口之一作为偏振控制编码器的输入端 36，另一端口经相位调制器 31 接 90 度旋转法拉第反射镜 30。一种略有变化但功能相同的结构是将延时线 33 与相位调制器 31（顺序无关）串接入同一端口，而另一端口仅连接一个 90 度旋转法拉第反射镜。工作时，光脉冲经可变分束器 32 的端口 36 进入可变分束器 32 分成两路，一路直接从可变分束器 32 的端口 35 直接输出，另一路经过延时线 33 延时，由 90 度旋转法拉第反射镜 34 反射回来，再经过可变分束器 32，再经过相位调制器 31 进行相位调制后经 90 度旋转法拉第反射镜 30 反射回来，反射回来的光脉冲经可变分束器 32 与上述直接输出的光脉冲合成一路由端口 35 输出，在对光脉冲进行分束时，控制可变分束器的分束比，使得由端口 35 输出的两个脉冲幅度相等，因两条光路均经 90 度旋转法拉第反射镜反射并经历各自的光路偶数次，所以由此输出的两个脉冲的偏振态相同。当延时线 33 和相位调制器 31（顺序无关）串接在同一端口，而另一端口仅连接一个 90 度旋转法拉第反射镜时，上述结果不受影响。脉冲从 35 端口输入，36 端口输出时结果相同。

实施例 7：

上述实施例中所列举的五种偏振控制编码器的组成结构中，相位调制器均可移动至输出光路中实现相同的相位调制功能。例如：一种相位调制器位于输出光路中的偏振控制编码器如图 5 所示，它由一个 2×2 的 3dB 分束器 18、两个 90 度旋转法拉第反射镜 20 和 22、一个相位调制器 19 和一个延时线 21 组成。其中 3dB 分束器 18 的一侧的两端口之一 16 作为偏振控制编码器的输入端，另一端口连接相位调制器 19 后作为偏振控制编码器的输出端 17，3dB 分束器 18 的另一侧的两端口之一连接 90 度旋转法拉第反射镜 20，同侧另一端口则顺序连接延时线 21、90 度旋转法拉第反射镜 22。所述的偏振控制编码器用于接收端时，上述位于输出光路的相位调制器必须移至脉冲分束前的输入光路，例如：偏振控制编码器 49-5 中的相位调制器 19 必须由串接在端口 17 改为串接在端口 16。工作时，光脉冲经分束器 18 的端口 16 进入分束器 18 分成两路，一路经过延时线 21 延时，由 90 度旋转法拉第反射镜 22 反射回来，另一路经 90 度旋转法拉第反射镜 20 反射回来，反射回来的两路光脉冲经分束器 18 合成一路由相位调制器 19 分别进行相位调制后再经端口 17 输出，因两条光路均经 90 度旋转法拉第反射镜反射并经历各自的光路偶数次，所以由此输出的两个脉冲的偏振态相同。当这种偏振控制编码器用于接收端时，上述位于输出光路的相位调制器 19 必须移至脉冲分束前的输入光路中，由相位调制器 19 对输入的两个光脉冲分别进行相位调制。

上述相位调制器位于发送端的输出光路中或位于接收端的输入光路中时对偏振保持特性没有要求。

实施例 8：

本发明的量子密钥分配装置中反向光子分离检测单元由：光学环行器 38 和单光子探测器 37 组成。其中，环行器的入射端口 39 作为反向光子分离检测单元的输入端口，环行器的出射端口 40 作为反向光子分离检测单元的同向输出端口，而从同向输出端口 40 入射的反向光子将被环行器 38 分离并导向单光子探测器 37 进行检测。如图 8 所示。工作时，从环行器的入射端口 39 输入的正向光子直接通过，由环行器的出射端口 40 输出，如果有光子从端口 40 反向进入反向光子分离检测单元，则环行器 38 将阻止该光子从端口 39 输出，而将该光子导向单光子探测器 37 检测，以判断是否有窃听木马光子存在，当将其用于接收端时，干涉后的信号光子的一路同样由探测器 37 检测，检测结果作为量子密钥信息使用。

实施例 9：

考虑到环行器和单光子探测器的工作波长范围有限，可能会有波长远离环行器和单光子探测器的光子反向进入偏振控制编码器，一种略有不同的反向光子分离检测单元如图 9 所示：其不同之处在于：输入端口 39 后增加一个光学带通滤波器 41。工作时光学带通滤波器 41 让系统工作波长范围内的光通过，而让反向光子分离检测单元工作波长范围以外的光子不能通过，增强系统抗窃听的能力。

实施例 10：

利用本发明的偏振控制编码器、反向光子分离检测单元以及单光子探测器、脉冲光源，可以组成一种典型的量子密钥分配系统如图 10 示：其中发送装置由单光子源 42（可由激光器和强衰减器组成的模拟单光子源替代）、本发明的偏振控制编码器 43、反向光子分离检测单元 44 组成。具体连接为：偏振控制编码器 43（可以是 49-1，49-2，49-3，49-6，49-7 或它们的变化型中的任一）的输入端与单光子光源 42 的输出端口连接，偏振控制编码器 43 的输出端则与反向光子分离检测单元 44（可以是 50-1，50-2 中的任一）的输入端连接，反向光子分离检测单元 44 的同向输出端口作为发送装置的信号输出端口与位于安全区外的量子信道 45 连接。

量子密钥分配系统的接收装置则由本发明的偏振控制编码器 47（可以是 49-1，49-2，49-3，49-6，49-7 或它们的变化型中的任一，其中 49-3 或 49-7 较好）、反向光子分离检测单元 46（可以是 50-1 和 50-2 中的任一）和单光子探测器 48 组成。具体连

接为：量子信道 45 进入接收安全区内与反向光子分离检测单元 46 的输入端连接，反向光子分离检测单元 46 的同向输出端与偏振控制编码器 47 的输入端连接，偏振控制编码器 47 的输出端则与单光子探测器 48 连接。

量子密钥分配方法是：发送者首先由单光子源 42 发送一个单光子脉冲（实际可以采用强衰减的脉冲激光代替，要求每个脉冲所含光子数不大于 1）进入偏振控制编码器 43，偏振控制编码器将单光子脉冲分束、相对延时、并对其中之一按量子密钥分配协议进行相位调制，输出偏振态相同的两个光脉冲通过反向光子分离检测单元 44 后进入量子信道 45 并单向传给接收装置；该两个光脉冲经过量子信道 45 到达接收装置后，先通过反向光子分离检测单元 46 进入偏振控制编码器 47，偏振控制编码器 47 再次将该两个脉冲分束、按量子密钥分配协议作相对延时、并按量子密钥分配协议进行相位调制；偏振控制编码器 47 输出的干涉信号之一直接送到单光子探测器 48 中检测（为降低暗计数和未相干部分的干扰，这里的检测需要采用时间门模式，门控信号可由发送端经典信道提供），偏振控制编码器 47 输出的干涉信号之二则通过反向光子分离检测单元分离后检测，根据上述两个干涉信号的检测结果、发送和接收方的相位调制记录以及双方公开对照的信息，并按照量子密钥分配协议的约定，即可得到一位量子密钥，重复上述过程，即可建立任意长度的无条件安全的量子密钥；由于偏振控制编码器内部采用偏振保持光路或 90 度法拉第旋转反射镜使得输出的两个光脉冲偏振态保持相同，因而系统具有很好的抗干扰能力。当发送和接收装置采用偏振控制编码器使用同一端口同时作为输入和输出端口时，光路中需要增加环行器、Y 型分束器等分束元件以分离输入和输出的信号；当发送和接收装置采用偏振控制编码器 49-6 和 49-7 时，在对光脉冲分束时需要控制分束比，使得输出的两个光脉冲幅度相等，以降低最终生成的量子密钥的误码率。

权利要求

1、一种偏振控制编码方法，其特征在于将入射的一个光脉冲分束为两个光脉冲，对二者作相对延时，再使这两个脉冲合成为一路输出，并在分束或合束后对其中的至少一个光脉冲按量子密钥分配协议进行相位调制，即编码；在分束到合束的过程中控制输出的两个光脉冲的偏振态，使得合束后输出的这两个光脉冲的偏振态相同。

2、如权利要求 1 所述的偏振控制编码方法，其特征在于所述使得输出的这两个光脉冲的偏振态相同的控制方法为：使所述两个光脉冲从分束到合束过程中的偏振态保持不变。

3、如权利要求 1 所述的偏振控制编码方法，其特征在于所述使得输出的这两个光脉冲的偏振态相同的控制方法为：使相对延时后的两个光脉冲分别经 90 度旋转法拉第反射镜反射奇数次，并经历分束到合束的各自的光路偶数次。

4、如权利要求 1 所述的偏振控制编码方法，其特征在于所述使得输出的这两个光脉冲的偏振态相同的控制方法为：使所述两个光脉冲之一直接输出，另一经 90 度旋转法拉第反射镜反射偶数次，并经历分束到合束的各自的光路偶数次。

5、根据权利要求 1 所述偏振控制编码方法构造的一种偏振控制编码器，其特征在于将一个光脉冲经过一个偏振保持分束器后分束成两个光脉冲沿两条光路传播，其中任一光路由延时线相对另一光路延时后再由偏振保持分束器合束成为一条光路输出，所述分束后的两条光路和合束后的输出光路三者中至少一路有相位调制器，所述偏振保持编码器的内部光路在分束到合束之间的部分是偏振保持光路。

6、根据权利要求 1 所述偏振控制编码方法构造的一种偏振控制编码器，其特征在于将一个光脉冲经过一个偏振保持分束器后分束成两个光脉冲沿两条光路传播，再由反射镜反射回来，其中任一光路的反射镜前加入偏振保持延迟线，使两条光路之间相对延时，并由原偏振保持分束器合束成为一条光路输出，所述分束后的两条光路和合束后的输出光路三者中至少一路有相位调制器，所述偏振保持编码器的内部光路在分束到合束之间的部分是偏振保持光路。

7、根据权利要求 1 所述偏振控制编码方法构造的一种偏振控制编码器，其特征在于将一个光脉冲经过一个分束器后分束成两个光脉冲沿两条光路传播，并由 90 度旋转法拉第反射镜反射回来，在其中任一光路中的 90 度旋转法拉第反射镜前加入延

迟线，使这两个光脉冲相对延时，再由原分束器合束成为一条光路输出，所述分束后的两条光路和合束后的输出光路三者中至少一路有相位调制器。

8、根据权利要求 1 所述偏振控制编码方法构造的一种偏振控制编码器，其特征在于将一个光脉冲经过一个偏振保持可变分束器后分束成两个光脉冲沿两条光路传播，一路直接输出，另一路由反射镜反射回来，并经过原偏振保持可变分束器后再由反射镜反射回来，再经过原偏振保持可变分束器与上述直接输出的光脉冲合束成为一条光路输出，所述反射镜前的两条光路中至少一个有延时线，所述反射镜前的两条光路和合束后的输出光路三者中至少一路有相位调制器，所述延时线与相位调制器在同一光路中时先后位置可以互易，所述偏振保持编码器的内部光路在分束到合束之间的部分是偏振保持光路。

9、根据权利要求 1 所述偏振控制编码方法构造的一种偏振控制编码器，其特征在于将一个光脉冲经过一个可变分束器后分成两个光脉冲沿两条光路传播，一路直接输出，另一路由 90 度旋转法拉第反射镜反射回来，并经过原可变分束器后再由 90 度旋转法拉第反射镜反射回来，再经过原可变分束器与上述直接输出光脉冲合束成为一条光路输出，所述反射镜前的两条光路中至少一个有延时线，所述 90 度旋转法拉第反射镜前的两条光路和合束后的输出光路三者中至少一路有相位调制器，所述延时线与相位调制器在同一光路中时先后位置可以互易。

10、一种量子密钥分配系统，其特征在于将从脉冲光源输出的一个光脉冲经发送端的偏振控制编码器分束成两个光脉冲沿两条光路传播，对二者作相对延时，再使这两个脉冲合束成一路输出，并对光脉冲按量子密钥协议约定进行相位调制，偏振控制编码器输出的这两个光脉冲经过量子信道单向传给接收端；接收端的偏振控制编码器将接收到的这两个光脉冲中的每个光脉冲分束成两个光脉冲组成的光脉冲组沿两条光路传播，对同组的这两个光脉冲按量子密钥协议约定作相对延时，再使这两个光脉冲组合束成一路输出，并对光脉冲按量子密钥协议约定进行相位调制，用单光子探测器同步检测这两个光脉冲组中的各至少一个光脉冲的叠加干涉结果，根据量子密钥分配协议进行量子密钥分配；当偏振控制编码器用于接收端且其中的相位调制器位于输出光路时，需将该相位调制器移至脉冲分束前的输入光路中。

11、如权利要求 10 所述的量子密钥分配系统，其特征在于在所述将发送端偏振控制编码器的出口或接收端偏振控制编码器的入口串接反向光子分离检测单元，该反向光子分离检测单元由光环行器和单光子探测器组成，其中光环行器的输入端接偏振

控制编码器的输出，环行器的同向输出端接量子信道，反向输出端接单光子探测器。

12、如权利要求 11 所述的量子密钥分配系统，其特征在于所述的反向光子分离检测单元中，光环行器的输入端串接一个光学带通滤波器。

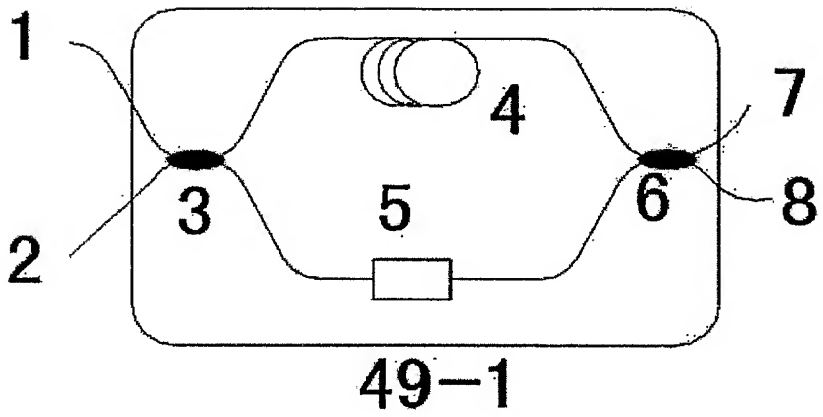


图 1

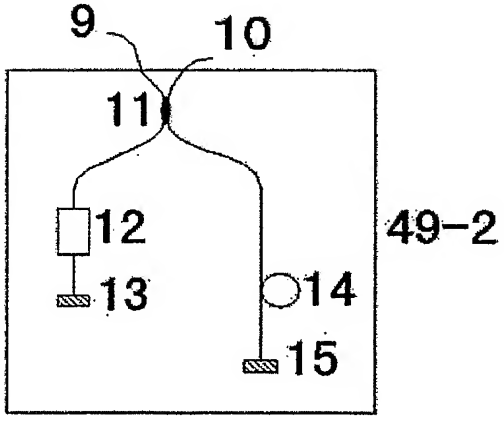


图 2

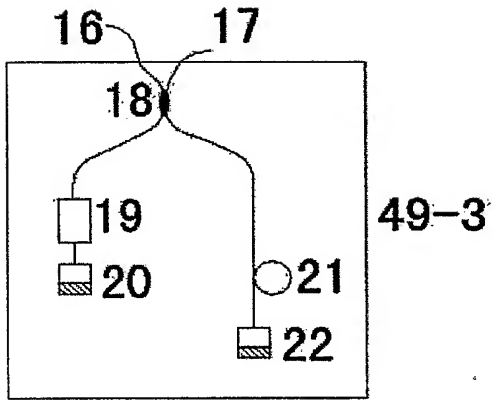


图 3

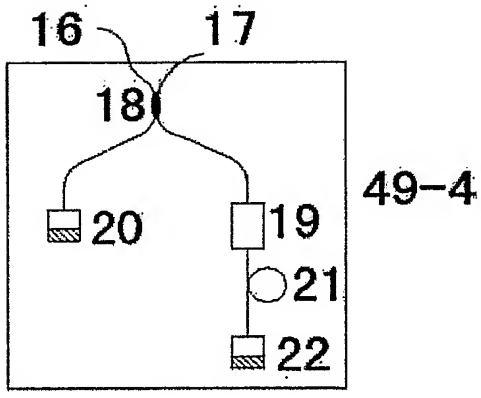


图 4

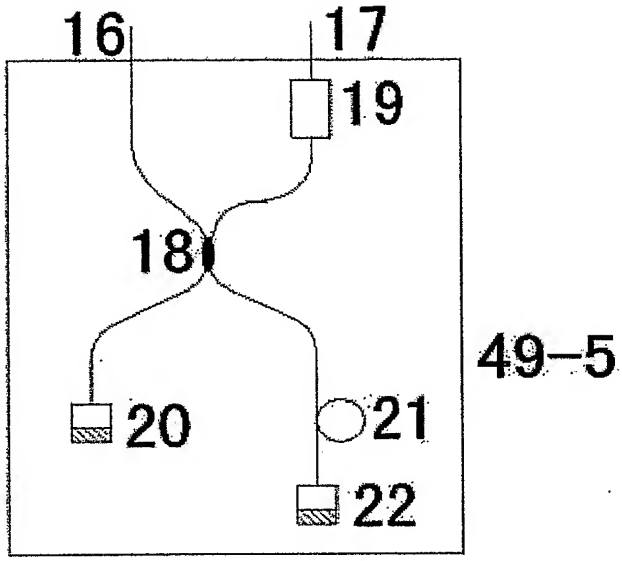


图 5

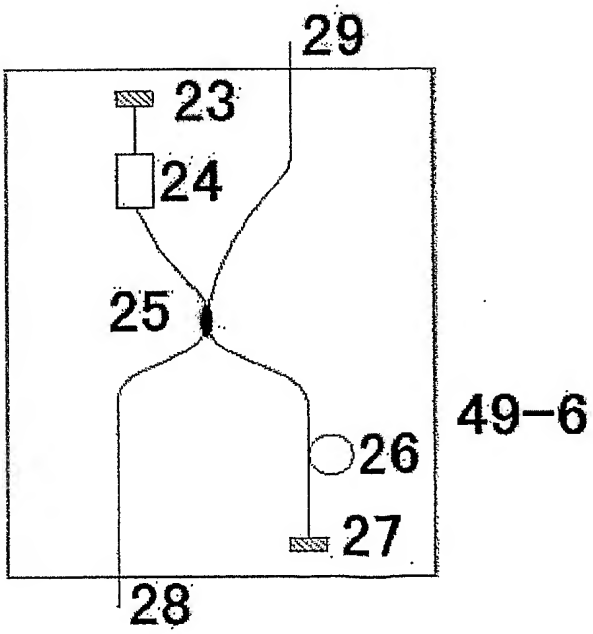


图 6

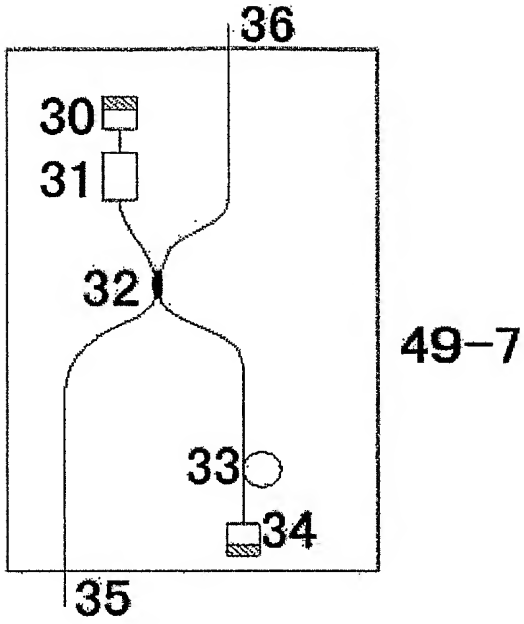


图 7

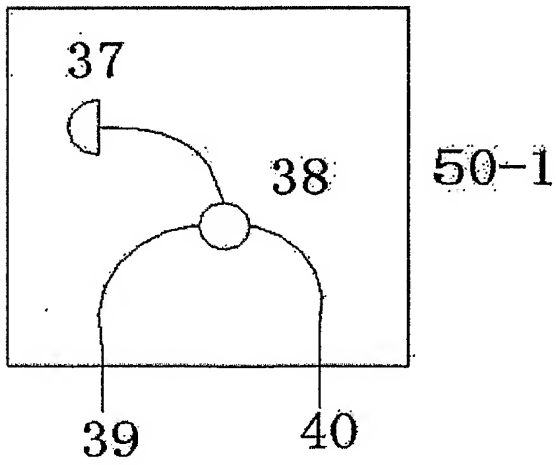


图 8

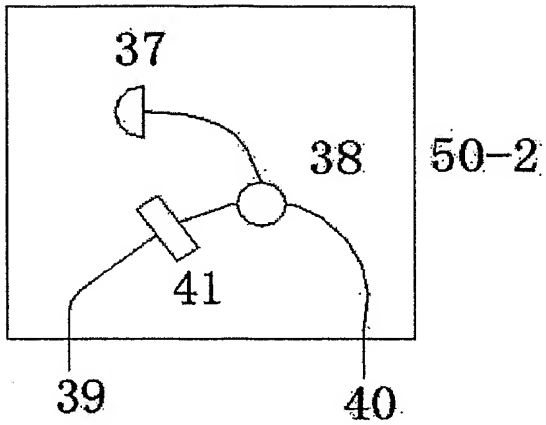


图 9

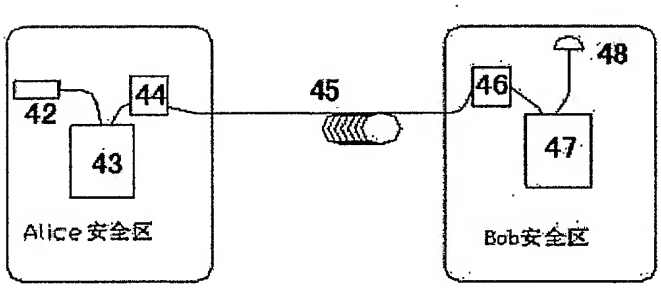


图 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2004/000969

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED G02B,H04L

Minimum documentation searched (classification system followed by classification symbols)

G02B26/08,H04L9/08,9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

CHINA JOURNAL

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

quantum w cryptogra+, quantum w key w distribut+, polariz+, polaris+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US6529601B1 (Paul D. Townsend, Ipswich (GB);04.Mar.2003,column4,line30 to column7,line50,Fig.1 to 4)	1、2、5—10
Y		4
X	US6438234B1(Nicolas Gisin, Geneva(CH) et al;20.Aug.2002,column2,line32 to column6,line 61,Fig.1 to 3)	1、3
X	US6188768B1(Donald Stimson Bethume, San Jose et al;13.Feb.2001,column3, line42 to column4,line35,Fig.1)	1
Y		4
X	CN1135820A((MINA) UK SEC FOR DEFENCE;(MINA) UK SEC STATE OR DEFENCE;12.Nov. 1996, page11, the last line to page13, the last	1
A	US5307410A(Charles H. Bennett, Croton-On-Hudson, N.Y.;26,Apr.1994,see the whole document)	1-12

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21.Apr.2005 (21.04.2005)	11 · MAY 2005 (11 · 05 · 2005)
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer MA, Yan Telephone No. (86-10)62085825

Form PCT/ISA /210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN 2004/000969

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
US6529601B1	2003.03.04	WO9744936A1	1997.11.27
		AU2906897A	1997.12.09
		EP0972373A1	2000.01.19
		JP2000511016T	2000.08.22
		CA2254767C	2002.04.16
US6438234B1	2002.08.20	CA2265553A	1998.03.12
		WO9810560A1	1998.03.12
		AU4206897A	1998.03.26
		EP0923828A	1999.06.23
		CZ9900477A3	1999.08.11
		JP2000517499TT	2000.12.26
		EP0923828B1	2004.01.28
		AT258733T	2004.02.15
		DE69727388EE	2004.03.04
		DK923828TT	2004.05.24
		ES2215238TT3	2004.10.01
US6188768B1	2001.02.13	None	
CN1135820A	1996.11.13	WO9510907A1	1995.04.20
		CA2173481A	1995.04.20
		EP0722640A1	1996.07.24
		GB2297448A	1996.07.31
		JP9505184TT	1997.05.20
		GB2297448B	1998.06.24
		EP0722640B1	1998.11.25
		DE69414874EE	1999.01.07
		ES2123825TT3	1999.01.16
		DE69414874TT	1999.05.12
		US6028935A	2000.02.22
US5307410A	1994.04.26	None	

Form PCT/ISA /210 (patent family annex) (April 2005)

国际检索报告

国际申请号
PCT/CN2004/000969

A. 主题的分类

H04L9/08

按照国际专利分类表(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域 G02B,H04L

检索的最低限度文献(标明分类系统和分类号)

G02B26/08,H04L9/08,9/00

包含在检索领域中的除最低限度文献以外的检索文献

中国期刊

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

EPODOC PAJ WPI CNPAT quantum w cryptogra+, quantum w key w distribut+, polariz+, polaris+

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	US6529601B1（Paul D. Townsend, Ipswich (GB);04.03 月 2003,第 4 栏第 30 行至第 7 栏第 50 行,图 1 至 4）	1、2、5-10
Y	同上	4
X	US6438234B1(Nicolas Gisin, Geneva(CH) et al;20.08 月 2002,第 2 栏第 32 行至第 6 栏第 61 行,图 1 至 3）	1、3
X	US6188768B1(Donald Stimson Bethune, San Jose et al;13.02 月 2001,第 3 栏第 42 行至第 4 栏第 35 行,图 1)	1
Y	同上	4
X	CN1135820A(大不列颠及北爱尔兰联合王国国防大臣;12.11 月 1996, 第 11 页最后 1 行至第 13 页最后 1 行, 图 7)	1
A	US5307410A(Charles H. Bennett, Croton-On-Hudson, N.Y.;26,4 月 1994,全文)	1-12

☐ 其余文件在 C 栏的续页中列出。 ☒ 见同族专利附件。

* 引用文件的具体类型：
"A" 认为不特别相关的表示了现有技术一般状态的文件
"E" 在国际申请日的当天或之后公布的在先申请或专利
"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件
"O" 涉及口头公开、使用、展览或其他方式公开的文件
"P" 公布日先于国际申请日但迟于所要求的优先权日的文件
"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件
"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性
"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性
"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
21.04 月 2005（21.04.2005）	11 · 5月 2005 (11 · 05 · 2005)
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号： (86-10)62019451	受权官员 马燕 电话号码：(86-10)62085825

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN 2004/000969

检索报告中引用的专利文件	公布日期	同族专利	公布日期
US6529601B1	2003.03.04	WO9744936A1	1997.11.27
		AU2906897A	1997.12.09
		EP0972373A1	2000.01.19
		JP2000511016T	2000.08.22
		CA2254767C	2002.04.16
US6438234B1	2002.08.20	CA2265553A	1998.03.12
		WO9810560A1	1998.03.12
		AU4206897A	1998.03.26
		EP0923828A	1999.06.23
		CZ9900477A3	1999.08.11
		JP2000517499TT	2000.12.26
		EP0923828B1	2004.01.28
		AT258733T	2004.02.15
		DE69727388EE	2004.03.04
		DK923828TT	2004.05.24
		ES2215238TT3	2004.10.01
US6188768B1	2001.02.13	None	
CN1135820A	1996.11.13	WO9510907A1	1995.04.20
		CA2173481A	1995.04.20
		EP0722640A1	1996.07.24
		GB2297448A	1996.07.31
		JP9505184TT	1997.05.20
		GB2297448B	1998.06.24
		EP0722640B1	1998.11.25
		DE69414874EE	1999.01.07
		ES2123825TT3	1999.01.16
		DE69414874TT	1999.05.12
		US6028935A	2000.02.22
US5307410A	1994.04.26	None	